

WHAT IS CLAIMED IS:

1. A communication device for communicating messages over a network comprising:

at least one transceiver, configured to transmit and receive a message having a message identifier and a plurality of recipient identifiers wherein the order of said plurality of recipient identifiers corresponds to an order of custody of said message by recipients, and wherein recipients are unable to edit said plurality of recipient identifiers.

2. The communication device of claim 1, further comprising a memory, configured to store a message log associating a transmitted message with said message identifier and with said plurality of recipient identifiers.

3. The communication device of claim 2, wherein:

said transceiver is further configured to receive, from a recipient of said message, an update of said message log.

4. The communication device of claim 1, wherein said transceiver is further configured to transmit and receive said message via a plurality of transport layer mechanisms.

5. The communication device of claim 1, wherein said transceiver is further configured to encapsulate said message in accordance with a protocol such that said message may be transmitted and received using said protocol.
6. The communication device of claim 1, wherein said transceiver is further configured to transmit a report to a message originator after transmitting said message wherein said message was previously received from said message originator.
7. The communication device of claim 1, wherein said transceiver is further configured to transmit a report to a message originator after transmitting said message wherein said message was previously received from a message recipient.
8. The communication device of claim 1, wherein said transceiver is further configured to receive, from a server, said message identifier and add said message identifier into said message prior to transmission of said message.
9. The communication device of claim 1, wherein said transceiver is further configured to transmit a report to a server after transmitting said message wherein said message was previously received from said message originator.
10. The communication device of claim 1, wherein said transceiver is further configured to transmit a report to a server after transmitting said message wherein said message was previously received from a message recipient.

11. The communication device of claim 1, wherein said transceiver is further configured to receive, from a server, an audit identifier and add said audit identifier into a message attachment prior to transmission of said message.

12. The communication device of claim 11, wherein said audit identifier uniquely corresponds to the combination of said message identifier, said order of said plurality of recipient identifiers, and a message originator identifier.

13. The communication device of claim 1, wherein said message comprises an encrypted message header that cannot be edited by recipients.

14. The communication device of claim 13, wherein said encrypted message header further comprises:

a message identifier field;

a message originator field; and

a recipient identifier field for containing said plurality of recipient identifiers.

15. The communications device of claim 14, wherein said encrypted message header further comprises a message expiration field.

16. The communication device of claim 14, wherein said recipient identifier field further comprises a flag field for indicating a message originator preference setting.

17. A server comprising:

a processor configured to assign and transmit a message identifier to a message originator communications device via a network; and

a memory configured to store a plurality of said message identifiers wherein each of said message identifiers is associated with a message transmitted by said message originator communications device.

18. The server of claim 17 wherein said processor is further configured to receive a message log update from a recipient communications device that had received said message.

19. The server of claim 18 wherein said processor is further configured to provide a message log report to a said message originator communications device.

20. A server comprising:

a processor configured to assign and transmit an audit identifier to a message originator communications device via a network; and

a memory configured to store a plurality of said audit identifiers wherein each of said audit identifiers is associated with a message attachment transmitted by said message originator communications device.

21. The server of claim 20 wherein said audit identifier uniquely corresponds to the combination of a message identifier, an order of recipient identifiers, and a message originator identifier.

22. The server of claim 21 wherein said audit identifier further comprises an identifier specific to said message attachment.

23. A method of communicating messages over a network comprising:
- embedding into a message a message identifier, message originator identifier, and message recipient identifier;
 - attaching content if any to said message;
 - preparing headers and suitable encapsulation of said message and said content in accordance with a communication protocol;
 - updating a message log; and
 - transmitting said message to a recipient using said communication protocol.
24. A method of tracking information custody comprising:
- receiving a message;
 - re-transmitting said message to at least one recipient; and
 - transmitting a message log update to a message originator.
25. The method of claim 24, wherein said message log update comprises a message identifier and a recipient identifier for said recipient.
26. A method of tracking information custody comprising:
- receiving a message;

re-transmitting said message to at least one recipient; and

transmitting a message log update to a server.

27. The method of claim 26, wherein said message log update comprises a message identifier and a recipient identifier for said recipient.

28. A method of constructing a message by a communications device comprising:

generating a message identifier;

adding said message identifier into a message header;

adding a message originator identifier to said message header;

adding at least one recipient identifier to said message header; and

encrypting said message header.

29. The method of claim 28, further comprising:

receiving from a server an audit identifier;

embedding said audit identifier into a message attachment; and

encrypting said message attachment.